



RECEIVED

DEC 19 2003

GROUP 3600

#1 S. K. R. E.

1 TITLE OF INVENTION

2 Retail Point of Sale (RPOS) Apparatus for Internet Merchandising

3 RELATED APPLICATIONS

4 Priority is claimed to provisional patent application submitted on June 30, 2000 under same
5 inventor's name, entitled Access Card for Internet Content (ACARD), provisional application number
6 60/215,673

8 FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

9 Not Applicable

11 SEQUENCE LISTING, TABLE, OR COMPUTER PROGRAM ON CD

12 Not Applicable

14 BACKGROUND OF INVENTION

15 (1) Field of the Invention

16 This invention relates generally to purchasing systems via a public computer network system
17 (Internet or World-Wide-Web). While the products sold on the Internet are often real and tangible, the
18 market place exists in a virtual realm. To conduct the business of selling in the virtual realm of the Internet,
19 a virtual transaction had to take place; or so it has been thought. This Invention requires non-virtual
20 transactions that take place at a retail point of sale for a means of virtual merchandising.

22 (2) Related Prior Art

23 Retail industries can exist anywhere. The historical version of retail was the actual retail point of
24 sale. A retailer established a store where customers could visit, look at merchandise and make purchases.

The customer had to visit the store in order to purchase the products. Other forms of retailing have existed like local street vendors, door-to-door salesmen, shop-by-telephone, mail order catalogs, in commercial shop-by telephone, and most recently, the Internet.

To understand the difference between this invention and prior art, one must first be able to understand the differences between retail point of sale and other methods of sale. There is always a time variable involved with merchandising transactions, but one should not make the mistake of assuming that time is the essential element that distinguishes between direct purchases and those on account. The basic formula for establishing a credit account is where the purchase price (P) of a product can be paid at a later time (T), an interest rate (R) can be assessed, and the amount paid $(A) = P(I + R)^T$.

A person may gain extra time to pay for a purchase by using credit, but it is the agreement between parties that one will extend credit to the other that creates a credit account. Time has no meaning in the direct purchase formula $(A) = P$. For that matter, there is always some lag between the time payment is tendered and possession takes place even if for just split seconds. Sometimes a lag between payment and possession requires a voucher so that the purchaser has some proof that payment has been made. The voucher is usually just a simple sales receipt. Other times it can be a ticket such as for attending a theater or other engagement. The voucher in this case does not represent an account or value of money. The voucher merely represents that the transaction has been completed and the merchandise, whether physical merchandise or simply entertainment, has been authorized.

Retail points of sale transactions involve at least one in-person contact with the buyer. On the Internet, it has always been assumed that this transaction must be conducted virtually on the Internet; after all, the Internet is a virtual realm. With the huge rise in popularity the Internet, there are rising concerns from the public about who should and who should not be able to access certain Internet content such as but not limited to: materials with copyrights such as music, content that is adult in nature, or other restricted access material.

49 Regulatory authorities and web masters have made attempts to control access through the selling of
50 access rights over the Internet itself. These services are often called subscription based I.D. or age
51 verification services. User names and passwords or other means of secure access have been delivered to
52 consumers after they entered credit card information. This has become an accepted means of control,
53 particularly with Adult Verification systems.

54 Public Key infrastructure (PKI) is one method that has evolved into a secure and anonymous means
55 of handling web transactions through the uses of encryption, trusted vendors, and trusted banking
56 institutions. PKI methods of Web transactions involve digital signature and money transactions over the
57 Internet. They require a customer, a bank, a merchant, a public archive such as an Internet web site,
58 Certificate Authorization servers, and encryption and decryption of the data.

59 Most secure web transactions require cookies and Web delivered applets (such as JAVA). A cookie
60 is information that a Web site puts on an end-users hard disk so that it can use the information at a later
61 time.

62 Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent
63 of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user
64 previously or anything about previous visits. A cookie is a mechanism that allows the server to store its own
65 information about a user on the user's own computer. For example, some browsers store cookies in a file
66 subdirectory and others store cookies as a single text file. Some computers employ programs to ensure that
67 cookies are not used and that the browser caching system will not keep a record of websites visited. A
68 programming sequence flow diagram for a cookie free cache back mini-application may look something
69 like this:

70 Secure On Routine

71 Make directory/temp/cachebak

72 Change directory/cachebak

73 Copy fat.db cachebak
74 Folder Copy Temporary Internet Files cachebak
75 Disable cookies in Internet Options settings
76 Disable JAVA
77 Secure Off Routine
78 Prompt user "download complete"
79 Compare fat.db to fat.db/cachebak
80 Compare Temporary Internet Files to Temporary Internet Files cachebak
81 Delete fat.db
82 Delete Temporary Internet Files
83 Copy cachebak fat.db to fat.db
84 Copy cachebak/Temporary Internet Files to Temporary Internet Files
85 Enable JAVA
86 END

87
88 Retail Point of Sale Apparatus (RPOS) For Internet Merchandising is a return to the simplistic
89 approach of pre-Internet ways of doing business, but it is not an obvious approach. As malicious attackers
90 of Internet communications become more common, the Internet security measures become increasingly
91 sophisticated. The RPOS takes away some of the sophistication and uses much simpler yet effective
92 technology in its place. The predefined transaction authorizes access to web content from a place off the
93 web, originates at a real place of business, and is a concept that a trained Internet professional may not be
94 able to grasp immediately; they have been conditioned towards more complicated means of accomplishing
95 the tasks directly on the Internet.

96 RPOS would not negatively affect any electronic commerce as it currently operates. It would
97 primarily be used in conjunction with current methods. A return to a retail establishment for conducting
98 Web business may hold great promise for Internet security in the future. A search of past practices and
99 inventions reveals a great deal of effort spent on avoiding over-the-counter transactions for Internet
100 e-commerce rather than embracing it as does the RPOS technology.

101 There are three key questions to be asked when attempting to differentiate the technology:

- 102 i. Do they take cash?
- 103 ii. Is there an establishment that acts on behalf of the customer for payment that employs non-
104 virtual (Retail point of sale) to complete the transaction?
- 105 iii. Does the customer have to physically go to the establishment to buy it?

106
107 The field of Internet e-commerce has numerous existing patents. A complete search for prior history
108 was not done prior to this filing but a few similar patents were found through a most basic search of the
109 on-line USPTO patent databases. They are reference below to help set the stage for one skilled in the art of
110 Internet commerce to understand the differences between RPOS and previous methods.

111 This invention is not a Prepaid Internet Access Card, such as used to supply the purchaser of
112 minutes on an Internet Service Providers (ISP) system, see US examples Patent Nos. 5,749,975; 5,987,612;
113 5,749,075, 5,987,430.

114 This invention is not merely a method for recording information on a card, computer disk, or other
115 means of recording, see US example Patent No. 6,076,733. The method of recording might be bar code,
116 magnetic tape, smart card, written inscription, or any means of recording information. This invention is not
117 used to locate a specific URL, but is used to divine the predetermined transaction that provided access to a
118 particular URL location.

119 This invention is not an organizational Internet access security system whereby business
120 organizations control access to web content of their own employees or to others on a closed network or to
121 generate personalized content pages for specific business purposes, see US Patent No. 6,076,166

122 This invention is not an Internet cash token system used as an anonymous means to get money to
123 spend on the Internet. See US examples Patent Nos. 6,076,078; 6,072,870; 6,061,660; 6,042,149

124 This invention is not electronic-voucher system, which places a third party URL as the guarantor of
125 funds. See US example 6,058,381.

126 This invention is not a mobile Internet media content delivery device in which the device itself
127 carries the content. See US examples Patent Nos. 6,018,720.

128 This invention is not a means to preview merchandise and set up an account to purchase - as in US
129 Patent No. 5,918,213, where the merchandise merely previewed at the point of sale, but then the transaction
130 is conducted as an off the shelf purchase, through typical Internet methods, or phone-in-sale automated
131 means. The retail point of sale apparatus for Internet Merchandising is a new means for conducting the
132 actual transaction that could be added to such a system.

133 This invention is not a device for delivering media content through on-line programmable smart
134 card authorization such as used in satellite television programming, or Web TV devices, where a home user
135 of the system can call in on the telephone to order Pay-per-view programming. In these systems the smart
136 card both receives and supplies data to the system over a private network. RPOS does not require
137 programming after the initial over-the-counter transaction.

138 Although the user of the RPOS may be known, it can also be used completely anonymously.

139

140 This invention is much like an event ticket to a movie theater or music concert except that the RPOS is
141 specifically used for access (entrance) to Internet merchandising.

142 While RPOS can facilitate Secure Web Transactions, it is not a method of the transaction, merely an
143 apparatus of divining the existence of a predetermined web transaction. It does not require a trusted vendor,
144 trusted bank, or buyer authentication. While RPOS may facilitate some of the same types of functions
145 mentioned above, it uses a completely new method.

146

147 BRIEF DESCRIPTION OF THE INVENTION

148 This invention is essentially retail point of sale for the Internet. In order to best set the stage for a
149 reader of this patent application to best understand the background of this invention and distinguish it from
150 prior art, several descriptive names of the invention are listed below. This is not intended to be an
151 exhaustive list but merely illustrates some of the ways such an invention can be used. After this list, for the
152 remainder of this document, the Invention will be referred to as the RPOS. Although it involves a voucher
153 system, the voucher need not exist in all circumstances. RPOS can use a disk, paper ticket, memory stick, or
154 any other means of supplying an access key and utility program.

155 Descriptive Names

- 156 1. Internet Content Voucher System
- 157 2. Cookie Free Cache Back System Card
- 158 3. Prepaid Card for Internet Content Media
- 159 4. Web Content Ticket
- 160 5. Over-the-counter Internet Sale
- 161 6. Simple Anonymity for Internet Content Delivery
- 162 7. Face-to-Face Verification System for Divining of Anticipated Internet Transaction
- 163 8. Non-Virtual Point of Sale for the Internet
- 164 9. Retail Point of Sale Card for Internet Content
- 165 10. Internet Authentication Card

11. Internet Adult Verification Card

12. Internet Allocation Card

The RPOS is an "actual point of sale" device for Internet content. Previous waves of invention attempting to satisfy the needs of secure web content on the Internet have delivered many "virtual point of sale" techniques and emphasis has been on the transaction itself and how to exchange money over the Internet.

When considering prior art, the RPOS invention differs most noticeably from previous methods in the way it does not follow the trend to do everything on the Internet and uses "actual point of sale" as the place where a predefined Internet sales transaction takes place. The information provided by web delivered cookies or applets is not required by RPOS because the information is already included; it is hand delivered to the computer by the user.

DESCRIPTION OF INVENTION

A security access key is provided in the form of a prepaid card sold as a retail item. The access key has a one time or multiple Internet session use as provided by the seller of the card. Through obtaining the CARD, the purchaser gains access to the website or specific web page(s) intended by the seller for either a defined duration of time or indefinite duration of time. Any time the end-user (customer) of the CARD is on the Internet, a very simple utility program may be deployed to ensure that there are no changes to the cache content of the customer's computer and no cookies are accepted or transmitted during the delivery of the media content. The utility of the invention is that it provides a method of controlling web access that requires at least one transaction be completed in person. No connection to a banking system for credit referencing is required, no vast system of computer networks is needed to verify anonymity and account

189 status. The actual transaction takes place over-the-counter. The delivery takes place on a computer of the
190 users choice.

191 The CARD is a voucher system that is used only to authenticate that the user of the card is in fact
192 the one in possession of it. The user of the CARD uses the card to access the content or merchandise from
193 the computer of their choice. As the time required for the user holding the card to receive the desired
194 content is decreased, the need for the CARD itself may become unnecessary. The content itself may be
195 recorded to disk compact disk, cassette, VHS tape, or other recording media: the media may be recorded at
196 the point of sale location.

197 The content that is recorded may be Internet content media or the content may be the purchase
198 agreement for merchandise. When the content is a purchase agreement for merchandise, the payment can be
199 made for the merchandise by the RPOS. The RPOS assumes responsibility for payment to the Internet
200 vendor and the purchaser specifies the shipping address of such merchandise.

201 Unlike any previous method of payment for Internet commerce in the past, there is no account,
202 credit, or other means of electronic payment required for the buyer in the transaction. The proof is within
203 the content itself. The content becomes the verification of a sale. Internet merchandisers may provide a
204 verification page for each sale, which they intend to be printed by the user. These types of verification pages
205 are excellent examples of specific URL information that can be determined ahead of time and sold whether
206 it is for merchandise or content media.

207 When the purchase is for non-prepackaged merchandise such as Content media, the media may be
208 individually licensed with a unique serial number for protection against counterfeiting. Content
209 fingerprinting is one of the methods used. Traditional digital signature may also be used.

210

211 Content Fingerprinting

212 Content fingerprinting could be used for printing secure documents, discouraging unauthorized use,
213 sending secret encoded messages, authentication of modification of documents, counterfeit detection, or
214 other application requiring secure distribution of Internet materials. Content fingerprinting differs from
215 digital signature or digital watermark in that the fingerprinting is not on the file itself but on the content of
216 the file.

217 In the Industry of Internet publishing, one of the problems has been unauthorized copying, posting
218 or otherwise revealing of sensitive materials for wide distribution. Millions of dollars in uncollected
219 royalties are lost each year. Publishers have no way of detecting the responsible parties who willfully post
220 the materials or otherwise "leak" the materials for wide distribution. The answer to the problem is a
221 mechanism or way to "mark" individual copies of recorded material for licensing so the publishers can feel
222 confident that appropriate royalties are being paid. The "mark" should be something not easily detected or
223 removed.

224 This document suggests just some basic methods of fingerprinting Internet content: Font
225 Fingerprinting, hidden pixelization, concealed ASCII and non-visible/inaudible codification.

226

227 Font Fingerprinting

228 Bar codes are typically comprised of black and white stripes, yet all that a bar code really represents
229 is a binary code. For Font Fingerprinting of Internet content, hidden binary codes are placed into documents
230 so that a specific record of the content travels with the document. It is much different from digital signature
231 for example where the file itself is tagged and encrypted and can't be read unless the proper keys are used to
232 decrypt the message. For fingerprint marking of the document, the mark stays with the document even after
233 it is properly received and possibly changed.

234 A base font is modified only slightly so as to not be immediately noticeable to the human eye, yet
235 enough for machine recognition. The base font becomes the "0" of the binary and the modified font is the

236 "1". Any text string can be modified to imprint a binary coded binary (BCB). The decoding is later
237 accomplished using a scanner with a character recognition system capable of distinguishing the font
238 differences.

239 Font fingerprinting is particularly designed to be most readily used for printed media, but the
240 fingerprinting could also follow a soft copied document provided the file format remains Rich Text Format
241 (.RTF) or better, giving access to the font aberrations. The font set used for printing the "fingerprinted"
242 document must also be available to the computer that receives the document. Future developments could
243 include a highly compressed file format capable of self-decompression that would mask the fact that the
244 Distributed font set is traveling with the document.

245 Another method of sending a font generated BCB with a softcopy document, not requiring a font
246 subset file, mixes two available fonts that are a close match such as Courier New with 11 point font and
247 Courier 10 BT with a 10 point font. While this combination is readily visible to the naked eye, the text is
248 not noticeably different unless you know what you're looking for. It was just an attempt at finding a good
249 match, but there may be other good system fonts that are a close enough match.

250

251 Hidden Pixelization

252 The format of choice for delivery of images over the Internet has been the jpeg, formally the ISO
253 standard 10918, which keeps the file size for delivery fairly small. All digital images of this type are made
254 up of tiny pixels. For hidden pixelization, a jpeg image is converted to a similar image of a higher
255 resolution (more pixels). In other words any single pixel in the original image is recreated as multiple pixels
256 all of the same color. For example a $320 \times 240 = 76,800$ -pixel image becomes a $640 \times 480 = 307,200$ pixel
257 image, or roughly four pixels per one pixel of the original image.

258 Several of the pixels from these new higher resolution images can then be encoded with a BCB by
259 varying the shades within the 4 pixels only slightly - leaving the neutral color of the original larger pixel

260 essentially unchanged. Any documents delivered over the Internet that contain these images are thereby
261 permanently marked.

262 This re-pixelization creates four available binary codes in the original pixel. The original color is the
263 "0" code and the slightly changed shade is the "1" of the binary. One of the keys to making this system less
264 detectable is to disguise the encoding by causing the encoded jpeg file to still report to the user that it is still
265 a 320 x 240 image when in fact it has been changed to a 640 x 480 image and then report back to the
266 viewing system the proper resolution. If the user resaves the image into a different format such as GIF, the
267 code may or may not be transferred, but as long as images in documents are untouched, the document
268 remains fingerprinted.

269

270 Concealed ASCII

271 ASCII stands for American Standard Code for Information Interchange. ASCII was developed a
272 long time ago and the characters are not always used in the same way on different computer systems. ASCII
273 was originally designed for teletypes and the first 31 characters in today's applications are no longer used as
274 originally intended. Concealed ASCII finger printing takes advantage of the fact that several of them act the
275 same as the ASCII character "032" in many applications. ASCII 32 is the code for a blank space.

276 ASCII characters 0, 10, and 13 do not display anything on most applications. Character 9 will move
277 to a tab, making a long blank space. 16-25 and 27-31 produce a black area on the screen in some
278 applications and a blank area in others. So do 1-9, 11, 12, 14, and 15 on some applications; however, they
279 often cause error messages in the compiler for many applications.

280 Concealed ASCII can create a BCB by using the standard ASCII 32 in spaces as the "0" character of
281 the binary and an alternate ASCII 0, 10, or 13 with ASCII 32 as the "1" character of the binary.

282 Example: The quick gray fox jumps over the lazy brown rabbit.

283 There are nine spaces to use for the BCB in the preceding phrase. The code in the example above
284 could read 010000111. The code for the 2nd, 7th, 8th, and 9th spaces in the phrase could be ASCII 10
285 followed by ASCII 32. The remaining spaces could simply use ASCII 32. While the concealed ASCII
286 fingerprinting is not printable, it can be used to travel with text of a printable document

287 Concealed ASCII can easily be lost when transmitted as plain text over the Internet and other
288 systemes, but many documents are transmitted over the Internet in specific file formats that would maintain
289 specific ASCII sequences not visible to the reader without looking to the particular codes that generated the
290 text.

291

292 Non-visible or Inaudible Codification

293 Analog signals of non-discernable frequencies for human ears or eyes are individually dubbed into
294 audio recordings, which can later identify the origin of the recording. The sights or sounds are created using
295 a frequency, signal generator, or other means of creating analog signals. The analog signals, which cannot
296 be heard by humans on the recording, can be used for distribution of copyright materials such as mp3 music
297 or dubbed into the soundtrack of a video that is distributed on the World-Wide-Web (Internet).

298 Identical songs or videos by the same artist can become individual versions that are licensed to
299 individuals. Using sensitive digital software and computer sound editing tools available from a number of
300 manufacturers the sights and sounds outside the range of human discernment can later be detected to verify
301 if the recording is in fact licensed and who is the owner of the license. The analog signals essentially encode
302 any individual identification to a song, video, or other media that contains audio or video tracks.

303 The human sound range is between 20 and 20,000 hertz for a young person and much less for an old
304 person. The human visual range for light lies within a range around 10⁹ MHz. Visual analog signals can
305 also be dubbed into digital video recordings. The key to non-visible or Inaudible Codification is merely that
306 that signals are dubbed into the content and not just on the file itself

Content Fingerprinting Usefulness

Fingerprinting documents is a useful and new idea. The usefulness of the specific methods shown here is greatly diminished when patented and the PTO discloses to the public. The actual methods of fingerprinting really should be kept as "Trade Secrets". The above methods are not fool proof or even sophisticated enough to hold up against even the least sophisticated of hackers. They are merely offered here as examples of how to individually license Internet materials. As industry looks to the Internet for delivery of every kind of copyrighted material, there will be other specific methods of fingerprinting. Fingerprinting Internet delivered media may involve documents, images, videos, sound tracks, or any other type of media that can be produced for the Internet.

Content fingerprinting is not just for watermarking content, it is capable of providing a level of security for transfer of ownership for prepaid media content over a public computer network (Internet). For example, Public Key Infrastructure (PKI) for secure and anonymous means of handling web transactions can be enhanced by variations of hidden content digital signature fingerprinting using visible or audible codes on a first mark on the content that is a first key of a first public/private key pair to indicate that said merchandise is authentic and a second label that is noticeable only by a machine as a second private key of a private/public key pair used to authenticate the delivery of merchandise.

DETAILED DESCRIPTION OF INVENTION

The following drawings provide examples of different applications and construct specifications for the RPOS technology. They are not meant to be inclusive of all uses, they are merely examples.

Figure #1 uses a flow chart to illustrate a use of the RPOS. The process begins with web content dealers who have content posted to a public computer network (Internet) and have chosen to use RPOS for distribution. The web content dealers may manufacture the card themselves or use a third party. The type of

331 security system used for placing the access key on the card is only important as to the particular level of
332 security that is desired. The web content dealer then distributes the CARD, directly or through distribution
333 channels, to a retail establishment. The retail establishment sells the CARD over the counter to the
334 customer. The dealer, distributor, and retail establishment may use whatever profit margins or price
335 mark-ups as they choose or is agreed upon. The CARD is delivered to the customer like any other retail
336 product. Continuing along the flow chart in Figure #1 to the customer, the CARD is used to access only the
337 web content that is predefined by the CARD. The purpose of the CARD in this transaction is only to ensure
338 that the user is in possession of it. The transaction takes place through an over-the counter sale.

339 Figure #2 uses a flow chart to illustrate an alternate use of the RPOS The process again begins with
340 Web Content Dealers. In this application the Web Content Dealers may or may not subscribe to the RPOS
341 system (i.e. make their own CARDS). To facilitate the creation of a CARD for the WEB Content Dealers, a
342 retail establishment supplies a computer or terminal as a customer access point, which provides Internet
343 access, and issues a CARD to a customer upon entering the retail establishment. The customer browses the
344 web and looks for content to purchase. Whenever a Web Content Dealer requires some sort of payment and
345 the customer agrees, the customer authorizes payment from the retail establishment and by default the retail
346 establishment agrees to the purchase. The customer is not required to enter his or her own name, credit card
347 payment information, address, or any other information that they do not choose. Upon leaving the
348 establishment, the customer pays the retail establishment the amount required for content received or to be
349 received. The purpose of the CARD in this transaction is only to ensure that the user is in possession of it.
350 The actual transaction takes place through an over-the-counter sale.

351 The system described in figure #2 illustrates a subtle yet important difference from prior art used in
352 Internet commerce, in that Internet access is only required for the customer to choose which media content
353 to purchase and to later retrieve on whatever computer the customer chooses. Internet access is not required
354 during the recording of specific media content locations (URLs); they can be simply written down, picked

355 out from a written menu after having seen the web dealers preview pages, or retrieved as a menu item from
356 the local computer at the check out. Internet access is also not required during the recording of the specific
357 access information, or during the retail transaction. While Internet Access during these processes may be
358 used to facilitate the RPOS processes, it is not required. While the CARD holds some intrinsic value it does
359 not hold any dollar amount information, account information, or other means of payment; the transaction is
360 completed in person at the checkout.

361 Figure #3 uses a flow chart to illustrate an alternate use of the RPOS. The process again begins with
362 Web Content Dealers. A Vending Machine Dealer purchases CARDS through normal product distribution
363 channels. Customer purchases the CARD from the vending machine acquiring the ability to access the
364 desired web content. This type of system is not capable of age verification as with over-the-counter sales.
365 Again, the purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The
366 actual transaction takes place through a vending machine.

367 Figure #4 illustrates how CARD is used as an age verification system (Adult Check). The process
368 begins with dealers of adult materials on the Internet. A retail establishment (such as video rental store,
369 convenience store, bookstore, adult merchandiser, or other type of store) obtains CARDS through typical
370 distribution channels. Customers purchase the CARD over the counter provided they can prove they are of
371 legal age to do so. Customer physically transports the CARD to a location where customer has access to a
372 computer that is capable of receiving Web content. The customer uses the CARD to obtain access to those
373 specific materials the seller of the CARD intended.

374 Figure #5 shows some examples of recording devices that are used or could be modified for use as
375 the media delivery method, access CARD, or to deliver a small cookie-free-cache-back application. Some
376 of these examples have also been patented previously. All that is required for use with the CARD is the
377 ability to deliver Personal Identification Number (PIN) information or other form of security used for
378 access. For optional added anonymity, the CARD may also deliver a small amount of software code to run

379 the mini-Application for Cookie Free Cache Back system. Reference 1 shows an example a of Low-level
380 security access key. Reference 2 shows an example of how a mini-application (applet) can be delivered on
381 floppy prior to accessing content. Reference 3 shows a better security system using a scratch off access key.
382 Reference 4 shows a smart card which could be used to deliver both an access key and mini-application
383 applet. In all of these examples the CARD is not used as money, credit, or cash.

384 Figure #6 is an example of Font Fingerprinting where a font subset file must be delivered to the
385 user.

386 Figure #7 is an example of Hidden Pixelization for Content Fingerprinting. The hidden pixelization
387 binary fingerprinting or encoded message can be divined using a scanning device capable of detecting the
388 differences.

389 Figure # 8 illustrates the similarities between the New Courier font and the Courier 10BT font.

1 TITLE OF INVENTION

2 Retail Point of Sale (RPOS) Apparatus for Internet Merchandising

3 RELATED APPLICATIONS

4 Priority is claimed to provisional patent application submitted on June 30, 2000 under same
5 inventor's name, entitled Access Card for Internet Content (ACARD), provisional application number
6 60/215,673

8 FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

9 Not Applicable

11 SEQUENCE LISTING, TABLE, OR COMPUTER PROGRAM ON CD

12 Not Applicable

14 BACKGROUND OF INVENTION

15 (1) Field of the Invention

16 This invention relates generally to purchasing systems via a public computer network system
17 (Internet or World-Wide-Web). While the products sold on the Internet are often real and tangible, the
18 market place exists in a virtual realm. To conduct the business of selling in the virtual realm of the Internet,
19 a virtual transaction had to take place; or so it has been thought. This Invention requires non-virtual
20 transactions that take place at a retail point of sale for a means of virtual merchandising.

22 (2) Related Prior Art

23 Retail industries can exist anywhere. The historical version of retail was the actual retail point of
24 sale. A retailer established a store where customers could visit, look at merchandise and make purchases.

Comment: Above headings are added
to help conform to USPTO recommended
content format.

Deleted: BACKGROUND

25 The customer had to visit the store in order to purchase the products. Other forms of retailing have existed
26 like local street vendors, door-to-door salesmen, shop-by-telephone, mail order catalogs, informercial
27 shop-by telephone, and most recently, the Internet.

28 To understand the difference between this invention and prior art, one must first be able to
29 understand the differences between retail point of sale and other methods of sale. There is always a time
30 variable involved with merchandising transactions, but one should not make the mistake of assuming that
31 time is the essential element that distinguishes between direct purchases and those on account. The basic
32 formula for establishing a credit account is where the purchase price (P) of a product can be paid at a later
33 time (T), an interest rate (R) can be assessed, and the amount paid (A) = $P(I + R)^T$.

34 A person may gain extra time to pay for a purchase by using credit, but it is the agreement between
35 parties that one will extend credit to the other that creates a credit account. Time has no meaning in the
36 direct purchase formula (A) = P. For that matter, there is always some lag between the time payment is
37 tendered and possession takes place even if for just split seconds. Sometimes a lag between payment and
38 possession requires a voucher so that the purchaser has some proof that payment has been made. The
39 voucher is usually just a simple sales receipt. Other times it can be a ticket such as for attending a theater or
40 other engagement. The voucher in this case does not represent an account or value of money. The voucher
41 merely represents that the transaction has been completed and the merchandise, whether physical
42 merchandise or simply entertainment, has been authorized.

43 Retail points of sale transactions involve at least one in-person contact with the buyer. On the
44 Internet, it has always been assumed that this transaction must be conducted virtually on the Internet; after
45 all, the Internet is a virtual realm. With the huge rise in popularity the Internet, there are rising concerns
46 from the public about who should and who should not be able to access certain Internet content such as but
47 not limited to: materials with copyrights such as music, content that is adult in nature, or other restricted
48 access material.

49 Regulatory authorities and web masters have made attempts to control access through the selling of
50 access rights over the Internet itself. These services are often called subscription based I.D. or age
51 verification services. User names and passwords or other means of secure access have been delivered to
52 consumers after they entered credit card information. This has become an accepted means of control,
53 particularly with Adult Verification systems.

54 Public Key infrastructure (PKI) is one method that has evolved into a secure and anonymous means
55 of handling web transactions through the uses of encryption, trusted vendors, and trusted banking
56 institutions. PKI methods of Web transactions involve digital signature and money transactions over the
57 Internet. They require a customer, a bank, a merchant, a public archive such as an Internet web site,
58 Certificate Authorization servers, and encryption and decryption of the data.

59 Most secure web transactions require cookies and Web delivered applets (such as JAVA). A cookie
60 is information that a Web site puts on an end-users hard disk so that it can use the information at a later
61 time.

62 Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent
63 of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user
64 previously or anything about previous visits. A cookie is a mechanism that allows the server to store its own
65 information about a user on the user's own computer. For example, some browsers store cookies in a file,
66 subdirectory and others store cookies as a single text file. Some computers employ programs to ensure that
67 cookies are not used and that the browser caching system will not keep a record of websites visited. A
68 programming sequence flow diagram for a cookie free cache back mini-application may look something
69 like this:

70 Secure On Routine
71 Make directory/temp/cachebak
72 Change directory/cachebak

Deleted: the Internet Explorer

Deleted: s

Deleted: Windows

Comment: Internet Explorer, Netscape, and Windows are Trademarks and should not be included in text of the specification

Deleted: . Netscape

Deleted: s

Formatted: Underline

73 Copy fat.db cachebak
74 Folder Copy Temporary Internet Files cachebak
75 Disable cookies in Internet Options settings
76 Disable JAVA
77 Secure Off Routine
78 Prompt user "download complete"
79 Compare fat.db to fat.db/cachebak
80 Compare Temporary Internet Files to Temporary Internet Files cachebak
81 Delete fat.db
82 Delete Temporary Internet Files
83 Copy cachebak fat.db to fat.db
84 Copy cachebak/Temporary Internet Files to Temporary Internet Files
85 Enable JAVA
86 END

Formatted: Underline

Comment: Precisely adapted from original disclosures in figure 5 drawing which was canceled by amendment

87
88 Retail Point of Sale Apparatus (RPOS) For Internet Merchandising is a return to the simplistic
89 approach of pre-Internet ways of doing business, but it is not an obvious approach. As malicious attackers
90 of Internet communications become more common, the Internet security measures become increasingly
91 sophisticated. The RPOS takes away some of the sophistication and uses much simpler yet effective
92 technology in its place. The predefined transaction authorizes access to web content from a place off the
93 web, originates at a real place of business, and is a concept that a trained Internet professional may not be
94 able to grasp immediately; they have been conditioned towards more complicated means of accomplishing
95 the tasks directly on the Internet.

Comment: Capitalization here was distracting in that it may have appeared to be another subject heading

Deleted: ETAIL POINT OF SALE APPARATUS

Deleted: OR INTERNET MERCHANDISING

96 | RPOS would not negatively affect any electronic commerce as it currently operates. It would
97 | primarily be used in conjunction with current methods. A return to a retail establishment for conducting
98 | Web business may hold great promise for Internet security in the future. A search of past practices and
99 | inventions reveals a great deal of effort spent on avoiding over-the-counter transactions for Internet
100 | e-commerce rather than embracing it as does the RPOS technology.

Comment: The U.S. patent and trademark office has changed how it handles computer related business methods, but that is not relevant to understanding and/or using this invention.

Deleted: The U.S. Patent and Trademark Commissioner announced that the Agency would be revamping its patent examination guidelines for computer-related inventions and e-commerce practices, see United States Patent and Trademark Office RIN 065 I-AB20.

101 | There are three key questions to be asked when attempting to differentiate the technology:

Comment: A separate subheading 3. Prior Art differentiated is not needed here.

Deleted: ¶
3. Prior Art Differentiated¶

- 102 | i. Do they take cash?
- 103 | ii. Is there an establishment that acts on behalf of the customer for payment that employs non-
- 104 | virtual (Retail point of sale) to complete the transaction?
- 105 | iii. Does the customer have to physically go to the establishment to buy it?
- 106 |

107 | The field of Internet e-commerce has numerous existing patents. A complete search for prior history
108 | was not done prior to this filing but a few similar patents were found through a most basic search of the
109 | on-line USPTO patent databases. They are reference below to help set the stage for one skilled in the art of
110 | Internet commerce to understand the differences between RPOS and previous methods.

111 | This invention is not a Prepaid Internet Access Card, such as used to supply the purchaser of
112 | minutes on an Internet Service Providers (ISP) system, see US examples Patent Nos. 5,749,975; 5,987,612;
113 | 5,749,075, 5,987,430.

Formatted: No underline

114 | This invention is not merely a method for recording information on a card, computer disk, or other
115 | means of recording, see US example Patent No. 6,076,733. The method of recording might be bar code,
116 | magnetic tape, smart card, written inscription, or any means of recording information. This invention is not
117 | used to locate a specific URL, but is used to divine the predetermined transaction that provided access to a
118 | particular URL location.

Formatted: No underline

119 This invention is not an organizational Internet access security system whereby business
120 organizations control access to web content of their own employees or to others on a closed network or to
121 generate personalized content pages for specific business purposes, see US Patent No. 6,076,166

122 This invention is not an Internet cash token system used as an anonymous means to get money to
123 spend on the Internet. See US examples Patent Nos. 6,076,078; 6,072,870; 6,061,660; 6,042,149

124 This invention is not electronic-voucher system, which places a third party URL as the guarantor of
125 funds. See US example 6,058,381.

126 This invention is not a mobile Internet media content delivery device in which the device itself
127 carries the content. See US examples Patent Nos. 6,018,720.

128 This invention is not a means to preview merchandise and set up an account to purchase - as in US
129 Patent No. 5,918,213, where the merchandise merely previewed at the point of sale, but then the transaction
130 is conducted as an off the shelf purchase, through typical Internet methods, or phone-in-sale automated
131 means. The retail point of sale apparatus for Internet Merchandising is a new means for conducting the
132 actual transaction that could be added to such a system.

133 This invention is not a device for delivering media content through on-line programmable smart
134 card authorization such as used in satellite television programming, or Web TV devices, where a home user
135 of the system can call in on the telephone to order Pay-per-view programming. In these systems the smart
136 card both receives and supplies data to the system over a private network. RPOS does not require
137 programming after the initial over-the-counter transaction.

138 Although the user of the RPOS may be known, it can also be used completely anonymously.

139

140 This invention is much like an event ticket to a movie theater or music concert except that the RPOS is
141 specifically used for access (entrance) to Internet merchandising.

142 While RPOS can facilitate Secure Web Transactions, it is not a method of the transaction, merely an
143 apparatus of divining the existence of a predetermined web transaction. It does not require a trusted vendor,
144 trusted bank, or buyer authentication. While RPOS may facilitate some of the same types of functions
145 mentioned above, it uses a completely new method.

Comment: The title of the invention includes apparatus, therefore RPOS should be referred to here as an apparatus, although method claims may still follow.

Deleted: method

147 BRIEF DESCRIPTION OF THE INVENTION

148 This invention is essentially retail point of sale for the Internet. In order to best set the stage for a
149 reader of this patent application to best understand the background of this invention and distinguish it from
150 prior art, several descriptive names of the invention are listed below. This is not intended to be an
151 exhaustive list but merely illustrates some of the ways such an invention can be used. After this list, for the
152 remainder of this document, the invention will be referred to as the RPOS. Although it involves a voucher
153 system, the voucher need not exist in all circumstances. RPOS can use a disk, paper ticket, memory stick, or
154 any other means of supplying an access key and utility program.

155 Descriptive Names

- 156 1. Internet Content Voucher System
- 157 2. Cookie Free Cache Back System Card
- 158 3. Prepaid Card for Internet Content Media
- 159 4. Web Content Ticket
- 160 5. Over-the-counter Internet Sale
- 161 6. Simple Anonymity for Internet Content Delivery
- 162 7. Face-to-Face Verification System for Divining of Anticipated Internet Transaction
- 163 8. Non-Virtual Point of Sale for the Internet
- 164 9. Retail Point of Sale Card for Internet Content
- 165 10. Internet Authentication Card

11. Internet Adult Verification Card

12. Internet Allocation Card

The RPOS is an "actual point of sale" device for Internet content. Previous waves of invention attempting to satisfy the needs of secure web content on the Internet have delivered many "virtual point of sale" techniques and emphasis has been on the transaction itself and how to exchange money over the Internet.

When considering prior art, the RPOS invention differs most noticeably from previous methods in the way it does not follow the trend to do everything on the Internet and uses "actual point of sale" as the place where a predefined Internet sales transaction takes place. The information provided by web delivered cookies or applets is not required by RPOS because the information is already included; it is hand delivered to the computer by the user.

Comment: No need to capitalize the word prior

Deleted: P

DESCRIPTION OF INVENTION

A security access key is provided in the form of a prepaid card sold as a retail item. The access key has a one time or multiple Internet session use as provided by the seller of the card. Through obtaining the CARD, the purchaser gains access to the website or specific web page(s) intended by the seller for either a defined duration of time or indefinite duration of time. Any time the end-user (customer) of the CARD is on the Internet, a very simple utility program may be deployed to ensure that there are no changes to the cache content of the customer's computer and no cookies are accepted or transmitted during the delivery of the media content. The utility of the invention is that it provides a method of controlling web access that requires at least one transaction be completed in person. No connection to a banking system for credit referencing is required, no vast system of computer networks is needed to verify anonymity and account

189 status. The actual transaction takes place over-the-counter. The delivery takes place on a computer of the
190 users choice.

191 The CARD is a voucher system that is used only to authenticate that the user of the card is in fact
192 the one in possession of it. The user of the CARD uses the card to access the content or merchandise from
193 the computer of their choice. As the time required for the user holding the card to receive the desired
194 content is decreased, the need for the CARD itself may become unnecessary. The content itself may be
195 recorded to disk compact disk, cassette, VHS tape, or other recording media: the media may be recorded at
196 the point of sale location.

197 The content that is recorded may be Internet content media or the content may be the purchase
198 agreement for merchandise. When the content is a purchase agreement for merchandise, the payment can be
199 made for the merchandise by the RPOS. The RPOS assumes responsibility for payment to the Internet
200 vendor and the purchaser specifies the shipping address of such merchandise. ↓

201 Unlike any previous method of payment for Internet commerce in the past, there is no account,
202 credit, or other means of electronic payment required for the buyer in the transaction. The proof is within
203 the content itself. The content becomes the verification of a sale. Internet merchandisers may provide a
204 verification page for each sale, which they intend to be printed by the user. These types of verification pages
205 are excellent examples of specific URL information that can be determined ahead of time and sold whether
206 it is for merchandise or content media.

207 When the purchase is for non-prepackaged merchandise such as Content media, the media may be
208 individually licensed with a unique serial number for protection against counterfeiting. Content
209 fingerprinting is one of the methods used. Traditional digital signature may also be used.

210

211 Content Fingerprinting

Comment: This sentence was originally included to further relate that this is just one embodiment of the invention. The language here may have been confusing or indefinite as to which "situation" this is referring to.

Deleted: The CARD in this situation may simply be a receipt of sale or other proof of payment.

Comment: Amazon, Barnes and Nobel, Buy.com, and Outpost are all trade names and should not be included in the text of the specification.

Deleted: such as but not limited to Amazon, Barnes and Nobel, Buy.com, Outpost, and others

212 | Content fingerprinting could be used for printing secure documents, discouraging unauthorized use,
213 | sending secret encoded messages, authentication of modification of documents, counterfeit detection, or
214 | other application requiring secure distribution of Internet materials. Content fingerprinting differs from
215 | digital signature or digital watermark in that the fingerprinting is not on the file itself but on the content of
216 | the file.

217 | In the Industry of Internet publishing, one of the problems has been unauthorized copying, posting
218 | or otherwise revealing of sensitive materials for wide distribution. Millions of dollars in uncollected
219 | royalties are lost each year. Publishers have no way of detecting the responsible parties who willfully post
220 | the materials or otherwise "leak" the materials for wide distribution. The answer to the problem is a
221 | mechanism or way to "mark" individual copies of recorded material for licensing so the publishers can feel
222 | confident that appropriate royalties are being paid. The "mark" should be something not easily detected or
223 | removed.

224 | This document suggests just some basic methods of fingerprinting Internet content: Font
225 | Fingerprinting, hidden pixelization, concealed ASCII and non-visible/inaudible codification.

226 |
227 | Font Fingerprinting

228 | Bar codes are typically comprised of black and white stripes, yet all that a bar code really represents
229 | is a binary code. For Font Fingerprinting of Internet content, hidden binary codes are placed into documents
230 | so that a specific record of the content travels with the document. It is much different from digital signature
231 | for example where the file itself is tagged and encrypted and can't be read unless the proper keys are used to
232 | decrypt the message. For fingerprint marking of the document, the mark stays with the document even after
233 | it is properly received and possibly changed.

234 | A base font is modified only slightly so as to not be immediately noticeable to the human eye, yet
235 | enough for machine recognition. The base font becomes the "0" of the binary and the modified font is the

Comment: Specification is giving examples of how content fingerprinting could be used, there is no claim limitation that suggest that these "would" be uses.

Deleted: w

Comment: The hypothetical browser security applet itself is not going to be claimed in the amended claims and therefore the reference to a particular GUI is also no longer needed in the specification.

Deleted: The Graphical User Interface (GUI) of the program uses two side-by-side text windows, One window is for the visible message and the other window is for the shorter encoded information, Once the two messages are input, the user clicks on a button for encoding which makes all the necessary adjustments to encode the hidden information into the visible message and saves to one file.¶

236 "I". Any text string can be modified to imprint a binary coded binary (BCB). The decoding is later
237 accomplished using a scanner with a character recognition system capable of distinguishing the font
238 differences.

Font fingerprinting is particularly designed to be most readily used for printed media, but the fingerprinting could also follow a soft copied document provided the file format remains Rich Text Format (.RTF) or better, giving access to the font aberrations. The font set used for printing the "fingerprinted" document must also be available to the computer that receives the document. Future developments could include a highly compressed file format capable of self-decompression that would mask the fact that the Distributed font set is traveling with the document.

245 Another method of sending a font generated BCB with a softcopy document, not requiring a font
246 subset file, mixes two available fonts that are a close match such as Courier New with 11 point font and
247 Courier 10 BT with a 10 point font. While this combination is readily visible to the naked eye, the text is
248 not noticeably different unless you know what you're looking for. It was just an attempt at finding a good
249 match, but there may be other good system fonts that are a close enough match.

250

251 Hidden Pixelization

The format of choice for delivery of images over the Internet has been the jpeg, formally the ISO standard 10918, which keeps the file size for delivery fairly small. All digital images of this type are made up of tiny pixels. For hidden pixelization, a jpeg image is converted to a similar image of a higher resolution (more pixels). In other words any single pixel in the original image is recreated as multiple pixels all of the same color. For example a $320 \times 240 = 76,800$ -pixel image becomes a $640 \times 480 = 307,200$ pixel image, or roughly four pixels per one pixel of the original image.

Several of the pixels from these new higher resolution images can then be encoded with a BCB by varying the shades within the 4 pixels only slightly - leaving the neutral color of the original larger pixel

Comment: The examples of the font aberrations would not likely survive the optical character recognition process when scanned into the USPTO database. Any examples of these aberrations should be included in the drawings portion of the application.

Deleted: ¶
Courier
New . abcdefghijklmnopqrstuvwxyz¶
Courier 10
BT: abcdefghijklmnopqrstuvwxyz
yz¶
Mixed:
. abcdefghijklmnopqrstuvwxyz¶
(this barcode reads
(010101010101010101010101)¶
¶

260 essentially unchanged. Any documents delivered over the Internet that contain these images are thereby
261 permanently marked.

262 This re-pixelization creates four available binary codes in the original pixel. The original color is the
263 "0" code and the slightly changed shade is the "1" of the binary. One of the keys to making this system less
264 detectable is to disguise the encoding by causing the encoded jpeg file to still report to the user that it is still
265 a 320 x 240 image when in fact it has been changed to a 640 x 480 image and then report back to the
266 viewing system the proper resolution. If the user resaves the image into a different format such as GIF, the
267 code may or may not be transferred, but as long as images in documents are untouched, the document
268 remains fingerprinted.

269

270 Concealed ASCII

271 ASCII stands for American Standard Code for Information Interchange. ASCII was developed a
272 long time ago and the characters are not always used in the same way on different computer systems. ASCII
273 was originally designed for teletypes and the first 31 characters in today's applications are no longer used as
274 originally intended. Concealed ASCII finger printing takes advantage of the fact that several of them act the
275 same as the ASCII character "032" in many applications. ASCII 32 is the code for a blank space.

276 ASCII characters 0, 10, and 13 do not display anything on most applications. Character 9 will move
277 to a tab, making a long blank space. 16-25 and 27-31 produce a black area on the screen in some
278 applications and a blank area in others. So do 1-9, 11, 12, 14, and 15 on some applications; however, they
279 often cause error messages in the compiler for many applications.

Comment: Windows is a trade name

Deleted: Windows

Comment: Windows is a trade name

Deleted: Windows

280 Concealed ASCII can create a BCB by using the standard ASCII 32 in spaces as the "0" character of
281 the binary and an alternate ASCII 0, 10, or 13 with ASCII 32 as the "1" character of the binary.
282 Example: The quick gray fox jumps over the lazy brown rabbit.

283 |There are nine spaces to use for the BCB in the preceding phrase. The code in the example above
284 |could read 010000111. The code for the 2nd, 7th, 8th, and 9th spaces in the phrase could be ASCII 10
285 |followed by ASCII 32. The remaining spaces could simply use ASCII 32. While the concealed ASCII
286 |fingerprinting is not printable, it can be used to travel with text of a printable document |
287 |Concealed ASCII can easily be lost when transmitted as plain text over the Internet and other
288 |systemes, but many documents are transmitted over the Internet in specific file formats that would maintain
289 |specific ASCII sequences not visible to the reader without looking to the particular codes that generated the
290 |text.

Deleted: s[

Deleted: is

Comment: The optical character recognition process for entering the specification into the USPTO database will not preserve any ASCII codes, therefor e "is" is replace by "could" or "could be."

292 Non-visible or Inaudible Codification

293 |Analog signals of non-discernable frequencies for human ears or eyes are individually dubbed into
294 |audio recordings, which can later identify the origin of the recording. The sights or sounds are created using
295 |a frequency, signal generator, or other means of creating analog signals. The analog signals, which cannot
296 |be heard by humans on the recording, can be used for distribution of copyright materials such as mp3 music
297 |or dubbed into the soundtrack of a video that is distributed on the World-Wide-Web (Internet).

298 |Identical songs or videos by the same artist can become individual versions that are licensed to
299 |individuals. Using sensitive digital software and computer sound editing tools available from a number of
300 |manufacturers the sights and sounds outside the range of human discernment can later be detected to verify
301 |if the recording is in fact licensed and who is the owner of the license. The analog signals essentially encode
302 |any individual identification to a song, video, or other media that contains audio or video tracks.

303 |The human sound range is between 20 and 20,000 hertz for a young person and much less for an old
304 |person. The human visual range for light lies within a range around 10⁹ MHz. Visual analog signals can
305 |also be dubbed into digital video recordings. The key to non-visible or Inaudible Codification is merely that
306 |that signals are dubbed into the content and not just on the file itself

307 Content Fingerprinting Usefulness

308 Fingerprinting documents is a useful and new idea. The usefulness of the specific methods shown
309 here is greatly diminished when patented and the PTO discloses to the public. The actual methods of
310 fingerprinting really should be kept as "Trade Secrets". The above methods are not fool proof or even
311 sophisticated enough to hold up against even the least sophisticated of hackers. They are merely offered
312 here as examples of how to individually license Internet materials. As industry looks to the Internet for
313 delivery of every kind of copyrighted material, there will be other specific methods of fingerprinting.

314 Fingerprinting Internet delivered media may involve documents, images, videos, sound tracks, or any other
315 type of media that can be produced for the Internet._

316 Content fingerprinting is not just for watermarking content, it is capable of providing a level of
317 security for transfer of ownership for prepaid media content over a public computer network (Internet). For
318 example, Public Key Infrastructure (PKI) for secure and anonymous means of handling web transactions
319 can be enhanced by variations of hidden content digital signature fingerprinting using visible or audible
320 codes on a first mark on the content that is a first key of a first public/private key pair to indicate that said
321 merchandise is authentic and a second label that is noticeable only by a machine as a second private key of
322 a private/public key pair used to authenticate the delivery of merchandise.

324 DETAILED DESCRIPTION OF INVENTION

325 The following drawings provide examples of different applications and construct specifications for the
326 RPOS technology. They are not meant to be inclusive of all uses, they are merely examples.

327
328 Figure #1 uses a flow chart to illustrate a use of the RPOS. The process begins with web content
329 dealers who have content posted to a public computer network (Internet) and have chosen to use RPOS for
330 distribution. The web content dealers may manufacture the card themselves or use a third party. The type of

Comment: Prior art search made by the patent examiner would suggest that watermarks have been used for copyright protection.

Deleted: Since, nobody is working on this type of copyright protection, the concept itself might be of strategic advantage.

Comment: This entire paragraph was added to support subject matter originally disclosed in the specification and at least in part within original claim 4 of the original application. The claims as filed in the original specification are part of the disclosure and, therefore, if an application as originally filed contains a claim disclosing material not found in the remainder of the specification, the applicant may amend the specification to include the claimed subject matter. In re Benno, 768 F.2d 1340, 226 USPQ 683 (Fed. Cir. 1985), see also MPEP 2163. The text of this paragraph was adapted directly from original claim 4 and the paragraph beginning at line 54 on page 3 of this document.

Formatted: Indent: First line: 0.5",
Line spacing: Double

Comment: Since the detailed description of the invention and drawings are intermingled here, there will be a slightly different subject heading.

Deleted: DRAWINGS

331 security system used for placing the access key on the card is only important as to the particular level of
332 security that is desired. The web content dealer then distributes the CARD, directly or through distribution
333 channels, to a retail establishment. The retail establishment sells the CARD over the counter to the
334 customer. The dealer, distributor, and retail establishment may use whatever profit margins or price
335 mark-ups as they choose or is agreed upon. The CARD is delivered to the customer like any other retail
336 product. Continuing along the flow chart in Figure #1 to the customer, the CARD is used to access only the
337 web content that is predefined by the CARD. The purpose of the CARD in this transaction is only to ensure
338 that the user is in possession of it. The transaction takes place through an over-the counter sale.

Deleted: A

339 Figure #2 uses a flow chart to illustrate an alternate use of the RPOS. The process again begins with
340 Web Content Dealers. In this application the Web Content Dealers may or may not subscribe to the RPOS
341 system (i.e. make their own CARDS). To facilitate the creation of a CARD for the WEB Content Dealers, a
342 retail establishment supplies a computer or terminal as a customer access point, which provides Internet
343 access, and issues a CARD to a customer upon entering the retail establishment. The customer browses the
344 web and looks for content to purchase. Whenever a Web Content Dealer requires some sort of payment and
345 the customer agrees, the customer authorizes payment from the retail establishment and by default the retail
346 establishment agrees to the purchase. The customer is not required to enter his or her own name, credit card
347 payment information, address, or any other information that they do not choose. Upon leaving the
348 establishment, the customer pays the retail establishment the amount required for content received or to be
349 received. The purpose of the CARD in this transaction is only to ensure that the user is in possession of it.
350 The actual transaction takes place through an over-the-counter sale.

Comment: There is no need to connect this sentence to a particular claim. The claims have been amended and the connection will no longer be valid.

Deleted: , which is the construct specification for claim 3 in this application.

351 The system described in figure #2 illustrates a subtle yet important difference from prior art used in
352 Internet commerce, in that Internet access is only required for the customer to choose which media content
353 to purchase and to later retrieve on whatever computer the customer chooses. Internet access is not required
354 during the recording of specific media content locations (URLs); they can be simply written down, picked

Comment: The apparatus shown in figure #2 is a more a system than a process, although method claims may still follow.

Comment: Better grammar

Deleted: processes

355 out from a written menu after having seen the web dealers preview pages, or retrieved as a menu item from
356 the local computer at the check out. Internet access is also not required during the recording of the specific
357 access information, or during the retail transaction. While Internet Access during these processes may be
358 used to facilitate the RPOS processes, it is not required. While the CARD holds some intrinsic value it does
359 not hold any dollar amount information, account information, or other means of payment; the transaction is
360 completed in person at the checkout.

361 Figure #3 uses a flow chart to illustrate an alternate use of the RPOS. The process again begins with
362 Web Content Dealers. A Vending Machine Dealer purchases CARDS through normal product distribution
363 channels. Customer purchases the CARD from the vending machine acquiring the ability to access the
364 desired web content. This type of system is not capable of age verification as with over-the-counter sales.
365 Again, the purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The
366 actual transaction takes place through a vending machine.

367 Figure #4 illustrates how CARD is used as an age verification system (Adult Check). The process
368 begins with dealers of adult materials on the Internet. A retail establishment (such as video rental store,
369 convenience store, bookstore, adult merchandiser, or other type of store) obtains CARDS through typical
370 distribution channels. Customers purchase the CARD over the counter provided they can prove they are of
371 legal age to do so. Customer physically transports the CARD to a location where customer has access to a
372 computer that is capable of receiving Web content. The customer uses the CARD to obtain access to those
373 specific materials the seller of the CARD intended.

374 Figure #5 shows some examples of recording devices that are used or could be modified for use as
375 the media delivery method, access CARD, or to deliver a small cookie-free-cache-back application. Some
376 of these examples have also been patented previously. All that is required for use with the CARD is the
377 ability to deliver Personal Identification Number (PIN) information or other form of security used for
378 access. For optional added anonymity, the CARD may also deliver a small amount of software code to run

Comment: There will be no claims to a security applet specifically. The term "helps" is replaced by "could be employed," which makes it an option of the apparatus and not a presumed embodiment of the apparatus. Original figure 5 was cancelled by amendment.

Deleted: Figure #5 is a flow chart for programming the small security application (cache back/cookie free) that helps control security and anonymity.¶

Deleted: 6

Comment: "the" is replaced by "a" again to explain the optional nature of any security applet that may be employed.

Comment: legend text that was deleted from originally submitted drawings

Deleted: the

379 the mini-Application for Cookie Free Cache Back system. Reference 1 shows an example a of Low-level
380 security access key. Reference 2 shows an example of how'a mini-application (applet) can be delivered on
381 floppy prior to accessing content. Reference 3 shows a better security system using a scratch off access key.
382 Reference 4 shows a smart card which could be used to deliver both an access key and mini-application
383 applet. In all of these examples the CARD is not used as money, credit, or cash.

Deleted: 7

384 Figure #6 is an example of Font Fingerprinting where a font subset file must be delivered to the
385 user.

Deleted: 8

386 Figure #7 is an example of Hidden Pixelization for Content Fingerprinting. The hidden pixelization
387 binary fingerprinting or encoded message can be divined using a scanning device capable of detecting the
388 differences.

Comment: Text precisely adapted from legend text deleted from original figure 7 by amendment.

389 Figure # 8 illustrates the similarities between the New Courier font and the Courier 10BT font.

Deleted: 9